Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.047132

ARTICLE

A Framework for Enhancing Privacy and Anonymity in Blockchain-Enabled IoT Devices

Muhammad Saad[1], Muhammad Raheel Bhutta[2], Jongik Kim[3,*] and Tae-Sun Chung[1]

[1]Department of Artificial Intelligence, Ajou University, Suwon, 443-749, Korea

[2]Department of Electrical and Computer Engineering, University of Utah Asia Campus, Incheon, 21985, Korea

[3]Department of Artificial Intelligence, Chungnam National University, Daejeon, 34134, Korea

*Corresponding Author: Jongik Kim. Email: jongik@cnu.ac.kr

Received: 26 October 2023 Accepted: 06 February 2024 Published: 26 March 2024

ABSTRACT

With the increase in IoT (Internet of Things) devices comes an inherent challenge of security. In the world today, privacy is the prime concern of every individual. Preserving one's privacy and keeping anonymity throughout the system is a desired functionality that does not come without inevitable trade-offs like scalability and increased complexity and is always exceedingly difficult to manage. The challenge is keeping confidentiality and continuing to make the person innominate throughout the system. To address this, we present our proposed architecture where we manage IoT devices using blockchain technology. Our proposed architecture works on and off blockchain integrated with the closed-circuit television (CCTV) security camera fixed at the rental property. In this framework, the CCTV security camera feed is redirected towards the owner and renter based on the smart contract conditions. One entity (owner or renter) can see the CCTV security camera feed at one time. There is no third-party dependence except for the CCTV security camera deployment phase. Our contributions include the proposition of framework architecture, a novel smart contract algorithm, and the modification to the ring signatures leveraging an existing cryptographic technique. Analyses are made based on different systems' security and key management areas. In an empirical study, our proposed algorithm performed better in key generation, proof generation, and verification times. By comparing similar existing schemes, we have shown the proposed architectures' advantages. Until now, we have developed this system for a specific area in the real world. However, this system is scalable and applicable to other areas like healthcare monitoring systems, which is part of our future work.

KEYWORDS

Privacy; anonymity; blockchain; IoT; smart contracts

1 Introduction

In the age of competitiveness, where there is an excessive need to record every point of the sphere through big data, the IoT has become an intrinsic part of the world. This increase has taken exponential growth over a period. With an enormous number of devices interacting, there come security challenges to keep the interactions safe [1]. These include the sensitive data shared across many platforms by

many stakeholders, and this valuable data needs to be secure from opponent takeovers. For this, many systems have been developed to come up with solutions to provide the required security.

One of the main concerns is the issue of privacy. Preserving privacy is an imposed challenge that needs to be taken care of [2]. Some mechanisms have evolved with time, but they are not completing the challenge of maintaining privacy. This concern is not only an individual's desired function but the present era's overall need. Privacy is one of the topmost priorities for the system, and this feature attracts more studies to focus on it. An additional challenge is maintaining the anonymity of the users across all platforms. There is a thin line that is often blurred between privacy and anonymity, but in the broader context of sensitive data, these two are different streams of study. Privacy is about the controlled sharing of information and can exist along a spectrum, allowing varying levels of disclosure. On the other hand, anonymity represents the extreme end of the privacy spectrum, where no identifying information is disclosed, and the individual remains completely concealed. Both functions are the focus of our research.

Blockchain is one of the new trending technologies. With its introduction in 2008 in Bitcoin by Satoshi Nakamoto, blockchain is being used in several fields other than cryptocurrencies and payment verification systems [3]. Because of its decentralized architecture and transparency, it is used in healthcare, transportation, and education areas. Systems requiring the third party as a prime player, cost a lot and have access to the whole data, are now shifting their focus toward this area [4]. As a distributed ledger technology, blockchain is widely used in trusted resource management [5]. Blockchain-based computing resource trading is established to guarantee security and privacy [6]. Smart contracts add another feature which attracts more research areas. In [7], the authors propose a blockchain-independent smart contract infrastructure suitable for resource constraint IoT devices.

Blockchain, being the new decentralized paradigm, is used in many fields. Research has been carried out in fields such as health care, cloud computing, edge computing, vehicular IoT networks, scale-free networks [8] and digital economy [9]. In [10], the authors propose a secure intrusion detection with blockchain based data transmission with classification model for cyber-physical system in health sector and the cloud storage in [11]. Cloud services and cryptographic cloud storage are discussed in [12], where the authors present comparisons between different existing methodologies. In [13], the authors propose an architecture for IoT sensors, producing high volume of data, and the processing at the edge that cannot be fulfilled by the resources available. In [14], the authors propose a novel decentralized key management for vehicular IoT networks to solve the problem of scalability. In [15], the authors discuss preserving privacy in the healthcare monitoring system by proposing an access control using blockchain. In [16], the authors propose a solution for preserving privacy through permissioned blockchain by allowing the authorities to check if the stored video, that is being shared, is unmodified.

Data verification system for CCTV surveillance camera in smart cities using blockchain is discussed in [17]. Blockchain usage in the energy sector is discussed in [18], where user friendly transaction time management is optimized. Blockchain combined with deep learning is also implemented in areas like disease screening systems [19]. In [20], the authors develop a method for disease information tracing with key components including information collection, and chain-cycle storage information query. In the knowledge-driven economy, intellectual property is an important asset. Patents registration and trading system is developed in [21] using blockchain. In [22], authors propose a service architecture enabled by the core functionalities of blockchain to record, secure, validate and track the original achievements registration and related transactions. Blockchain can further be

applied to different areas where the architecture is already developed, for instance, model for textual sentiments of user reviews and ratings in [23] and online shopping in [24].

Security and privacy are the core challenges in the IoT area. To deal with them, blockchain is used as a backbone in various architectures [25,26]. The use of blockchain not only reduces the power of a central authority but also provides all the stakeholders of the system with equal opportunity to make decisions. Existing challenges and shortcomings in the blockchain framework, i.e., Privacy and anonymity, are the main motivations behind this research work. Most studies focus on either privacy [27,28] or anonymity [29,30].

In [31], the authors propose an architecture that addresses both the privacy and anonymity features. They adopt the K-anonymity method in constructing a united request to hide the location information of Electric Vehicles (EVs) based on undirected graphs. The limitation of this scheme is the use of consortium blockchain, where there are some controlling nodes to verify and validate the transactions. The attacker in this scheme can get the location coordinates of EVs though it is hard to distinguish which EV the coordinate belongs to. Our proposed framework adopts separate portions to preserve privacy and maintain anonymity and has better privacy preservation though the use of single key usage at a time. Furthermore, anonymity is maintained by modifying the existing cryptographic technique which adds a further concealing layer. Another advantage of our proposed framework is its simple architecture based on complex techniques.

Using Blockchain as a backbone technology for IoT systems is a common practice these days. Due to the distributed nature of our design and the need to preserve privacy and anonymity in the system, we have used this technology. Our design is scalable without limit, which blockchain is easily capable of due to its decentralized nature. The system holds sensitive monetary transactions and there are strict contractual agreement issues involved in our design which are handled by blockchain attributes very smoothly. Furthermore, to avoid the cases of forgery, both by the owner and the renter, this system is implemented using smart contract and key management.

To achieve privacy and anonymity, we propose a blockchain design for the CCTV security camera rental system. The main contributions of our work our summarized as follows:

- The blockchain based framework is proposed that works by using a single key at one time and invalidating the old keys to avoid forging in the system. This framework is scalable to larger systems and other areas like healthcare monitoring, automotive industry, and the like.
- A novel smart contract algorithm is devised to run the system abiding by all the rules and restricting the entities in the system within their jurisdictions. It dictates all the conditions of the system and triggers the conditions whenever something is changed in the system like a new tenant comes or a housing contract expires.
- A new mechanism for anonymity is introduced modifying the original ring signature and amending it to cater to our system's requirements. By introducing this modification, anonymity is further enhanced.

The remainder of this paper is organized as follows: Section 2 reviews the related work. The proposed framework architecture is explained in Section 3. Theoretical analyses are discussed in Section 4 along with the comparisons, while Section 5 concludes the paper with future research directions.

2 Related Works

There have been various studies about ensuring anonymity and preserving privacy in the blockchain system. Each proposed scheme has different limitations which make it less effective for the following mechanism. Studies prove that ensuring anonymity in the blockchain system is a hard task. Privacy, on the other hand, has been dealt with more than anonymity, but the loopholes and challenges remain.

In [29], the authors propose a design of communication and transaction anonymity in blockchain-based transactive microgrids. They proposed Privacy-preserving Energy Transactions (PETra) solution that preserves prosumers' (Producers and consumers) privacy. Fig. 1 shows the proposed PETra architecture and step-by-step execution. There is on-and-off blockchain communication. Before every transaction, both at the seller's end and the buyer's, the assets are checked if the person performing the transaction is capable enough (have energy asset as a seller or monetary asset as a buyer). The transaction is then signed by the prosumers, and the transaction is recorded on the blockchain. The authors present the solution in the form of ring signatures [32] and zero-knowledge proofs [33]. The solution works by mixing through both cryptographic techniques. This scheme has limitations concerning the risk of identifying, linking, and tracing transactions. Compared to this, our framework is more robust towards preserving privacy as we use unique key usage scenarios and key invalidation features.

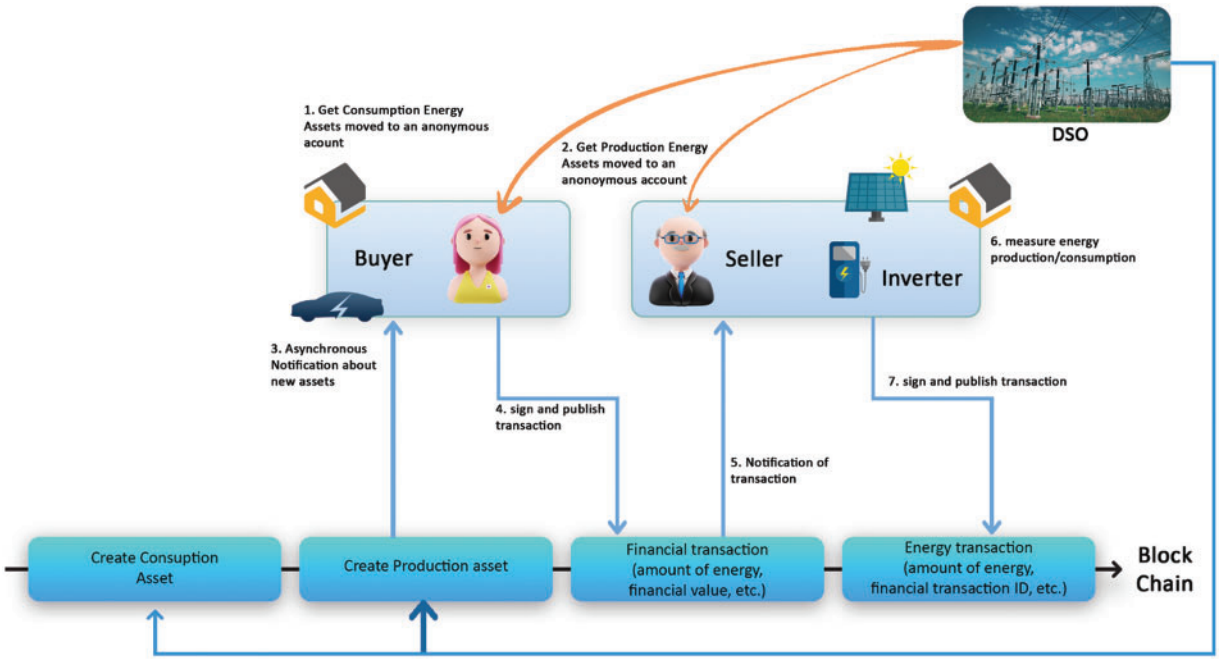

Figure 1: Privacy-preserving Energy Transactions (PETra) architecture

In [34], the authors present a unique way of ensuring anonymity. They present the Privacy respecting Contracts (PrC). They use stealth addresses and create the proxy user and proxy owner when renting a property. Blockchain is used to nullify the need for any third parties to overlook the whole system. Fig. 2 represents the working of PrC and how stealth addresses are used instead of real addresses to mask the actual identities. The authors used zk-SNARK (zero-knowledge Succinct Non-interactive Argument of Knowledge) Proofs [35]. The owner' and User' are the proxies that hide

the original identities. Analysis shows that the issue of double usage is avoided, and owner and user privacy is preserved due to the two-step procedure. The authors also provided the performance analysis of blockchain and cryptographic primitives, which shows the time taken by different operations. The main limitation of this scheme is that the two-layer approach applies to simple problems, but with complex systems, the operations and identity recovering capabilities are compromised. Our proposed architecture works better than this scheme in anonymity aspect as we use the ring signatures.

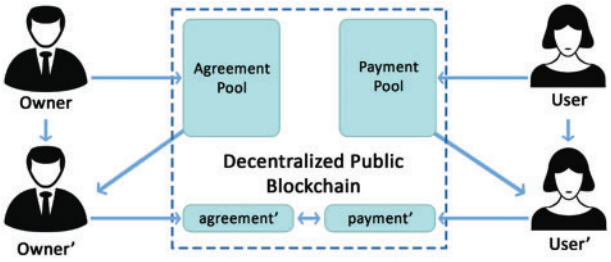

Figure 2: Privacy respecting Contracts (PrC) architecture

Different researchers come up with different schemes to ensure anonymity in the system. In [36], ring signatures are used with various changes, and they have proposed different versions of ring signatures suitable to different systems. In [37], the authors discuss different areas where ring signatures have been used, like oracle systems and electronic cash. In [38], the authors propose a video surveillance system based on blockchain. The architecture encrypts and stores the video, creates a license within the blockchain, and exports the video. The decryption key for the video is managed by the private DB of the blockchain. Though the scheme fulfils the security task, there comes a limitation in the form of speed of the network due to the decryption key stored separately.

In [39], the authors propose a framework for privacy in blockchain-enabled IoT devices. The authors give an overview of a rental room system where the CCTV camera feed needs to be private and directed to the renter only instead of the owner. There is the role of the third party as a manufacturer, and the authors use smart contracts to make the system automated. In [40], the authors extend this work and give the implementation in smart contract on the Ethereum platform. Fig. 3 shows the working of the CCTV camera feed system in a rented place ensuring privacy. The public keys used in this scheme are the IP addresses of the owner, the renter, and the CCTV camera. There is no mechanism given for renewing the addresses when the renter is changed and no option for extending the rental contract. Compared to this, our framework performs better towards preserving privacy, key usage, and ensuring anonymity. This architecture is the basis for our proposed design with the introduction of a novel smart contract algorithm.

Compared to all the existing schemes, our proposed scheme achieves the desired targets of maintaining privacy, keeping anonymity intact, exterminating the need for third-party services, and using smart contracts. Our framework can be compared to any existing system that can eliminate security threats in IoT-enabled devices be it the risk of tracing transactions in PETra or the two-layered structure of the PrC.

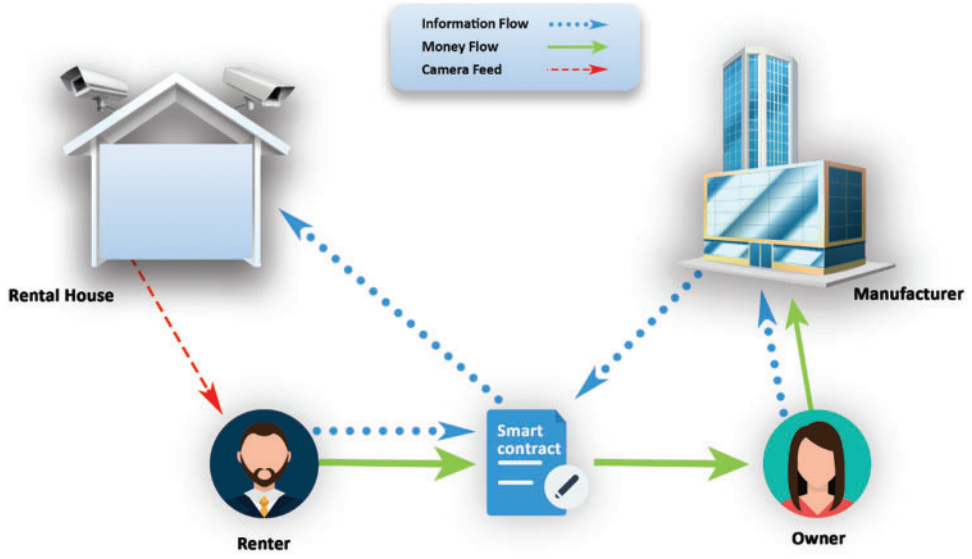

Figure 3: Privacy-preserving (PP) CCTV camera architecture

3 Proposed Architecture

Our target system is the CCTV security camera rental system, where the camera feed can be seen by the property owner or the renter one at a time. This system needs an extensive level of preserving privacy and maintaining anonymity. Consider the system of CCTV security camera at a rental property [41]. The renter desires a level of privacy that is not infringed by anyone, so the owner of the property should not be able to see the camera feed. Another scenario is the smart school system, where parents can pay to rent CCTV security cameras in the classrooms to see the teaching system. The parents would want to stay anonymous about who is watching the video stream. One more scenario where this architecture can be implemented is, a big company having different stakeholders and every stakeholder having a team of workers. The CCTV security camera can be rented out by stakeholders to see the working ethics of all the employees. In all these scenarios, the common thing is the desire for privacy and remaining anonymous.

This section is organized as follows: In Section 3.1, we briefly introduce blockchain technology. Section 3.2 will describe the basic architecture of our proposed system. While presenting the overall architecture of our system, we will detail our approach to preserving privacy using a single key at one time. In Section 3.3, we will develop a novel smart contract algorithm that enables our approach to privacy preservation by abiding by all the rules and restricting the entities in the system within their jurisdictions. In Section 3.4, we propose a modified ring signature for key management, which enables us to achieve anonymity.

3.1 Overview of Blockchain

Blockchain is the distributed database of records of all transactions of digital events executed and shared among participating parties. It contains every single record of each transaction. Some systems require dependency on a third party, like P2P payments, and are also sensitive about data privacy. In those systems, blockchain is the perfect fit. It ensures immutability and decentralization. Smart contracts [42] are another vital part of blockchain, which is important for our system. Anonymity and privacy are the inherited challenges in the blockchain system [43]. Anonymity means that the original

sender remains innominate. Privacy, on the other hand, refers to the transaction mostly and the content of the message which brings upon the challenge of adversaries making the system hacked [29].

3.2 Basic Architecture of the Proposed System

We call our system Secure Privacy and Anonymity Setup (SPAS). We have incorporated blockchain technology into our system by utilizing its basic principles. The technology's distributed nature enables each participant of the network to access the entire database and its history to avoid forgery. There is no single point of failure, and data remains protected. Peer-to-peer transmission limits the dependence on the third party for central operations. This ensures that the transaction is conducted directly between the stakeholders. Immutability ensures that there is no double usage, e.g., the renter cannot rent multiple properties with the same amount, and the owner cannot rent the same property to multiple renters. Immutability also ensures that there is no reversal of transactions, and nothing can be changed in history. Smart contracts dictate the rules and conditions governing the whole architecture.

The six entities in SPAS are: The security agency, the owner of the property, the renter, the web portal, the smart contract, and the CCTV security camera. The security agency is responsible for deploying the camera, and its role is restricted to requesting keys generation when needed. The owner is the one who owns the property and the CCTV security camera. There can be many owners in the network, each having multiple properties with a single CCTV security camera at each property. The renter is the person who rents the property for a specific time. A web portal is a security agency's interface that the renter uses to validate the keys and execute the expiration method. Smart contracts are an essential part comprising the policies defined. All six entities have their distinct role in making the whole scheme work together. One of the highlights of SPAS is, using a single key at one time, either with the owner or the renter, and the invalidation of previous keys. Through this, the security risk of re-using the keys is eliminated. Due to this, no chance is left for the unpaid CCTV security camera stream to the renter. Another one is transparency, which is ensured with the use of smart contracts. Smart contracts cannot be changed once made with specific conditions, so no one can cheat by extending the rental duration or forging the conditions [44].

Fig. 4 shows the basic architecture of SPAS. There is both on-blockchain and off-blockchain communication. On-blockchain communication is carried out through the smart contract, which contains information about the owner and the renter, the policies behind the scheme's working, and the scenarios for making different decisions based on the input from the user. This contract starts working from the time the security agency deploys the CCTV security camera. It is the communication channel between the owner and the security agency, the owner and the renter, and the security agency and the renter, as all accounts are made on the security agency's blockchain network. Off-blockchain communication is carried out between the owner and the CCTV security camera, the owner and the renter, and the web portal and the renter, where a renter generates a temporary ID for verification to get the CCTV security camera access.

The owner, renter and the security agency have roles both on-and-off blockchain. The security agency is the originator of the whole system. It creates its blockchain network on the existing Ethereum platform. This is a private blockchain whose members are the customers of the security agency that is handling all the CCTV security cameras. The security agency creates a smart contract and invites the owner and the renter to enter their details in smart contract. The owner and renter both generate their public and private keys through symmetric key encryption and enter the public keys and remaining details into smart contract. The rental contract is now complete and the handing over of the property

takes place. Prior to this, the money is transferred to the owner and the transaction is encrypted through a modified ring signature to mask the identity of both the owner and the renter. The design works in three main parts: (1) Deployment and smart contract creation, (2) Renting property, and (3) Expiration of rental contract.

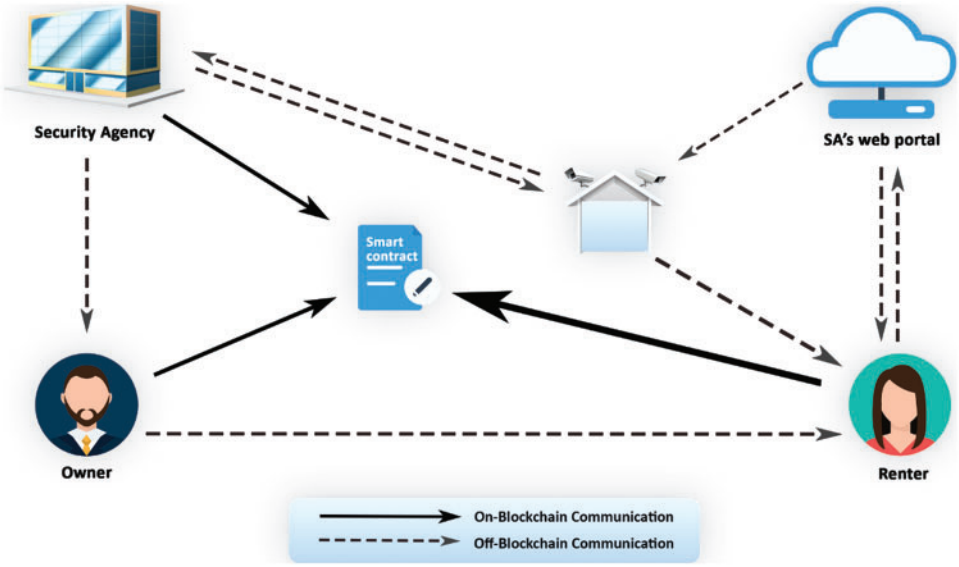

Figure 4: Secure Privacy and Anonymity Setup (SPAS) architecture

3.2.1 Deployment and Smart Contract Creation

In SPAS, security agency's role is limited to CCTV security camera deployment and maintenance services. The agency is not allowed to monitor the feed of CCTV security cameras. Fig. 5 shows the sequence of our proposed scheme's first part. After the deployment of the CCTV security camera, the security agency prompts the owner to create a blockchain account on its blockchain network, which already has multiple owners owning multiple properties. The owner creates his account and keeps the account keys. The security agency creates a smart contract and creates an owner's field to be filled by the owner. The owner fills in the information, including the blockchain account address and a public key to receive the camera feed. The security agency then asks the CCTV security camera to generate public and private keys and send the public key of the camera to the owner.

3.2.2 Renting Property

Fig. 6 shows the sequence of renting a property. When renting the property, the owner asks the renter to create a blockchain account on the security agency's blockchain network, which already contains multiple renter accounts. The renter creates the blockchain account and generates the key pair. The blockchain address is entered into the smart contract by the renter. The renter enters their remaining information, including the phone number and the public key. After the information is entered, a temporary ID is generated, and sent to the renter to enter it on the security agency's web portal. If the entered temporary ID is matched and verified, the web portal marks the access flag on the CCTV security camera as 'true' and asks the CCTV security camera to generate the new key pair.

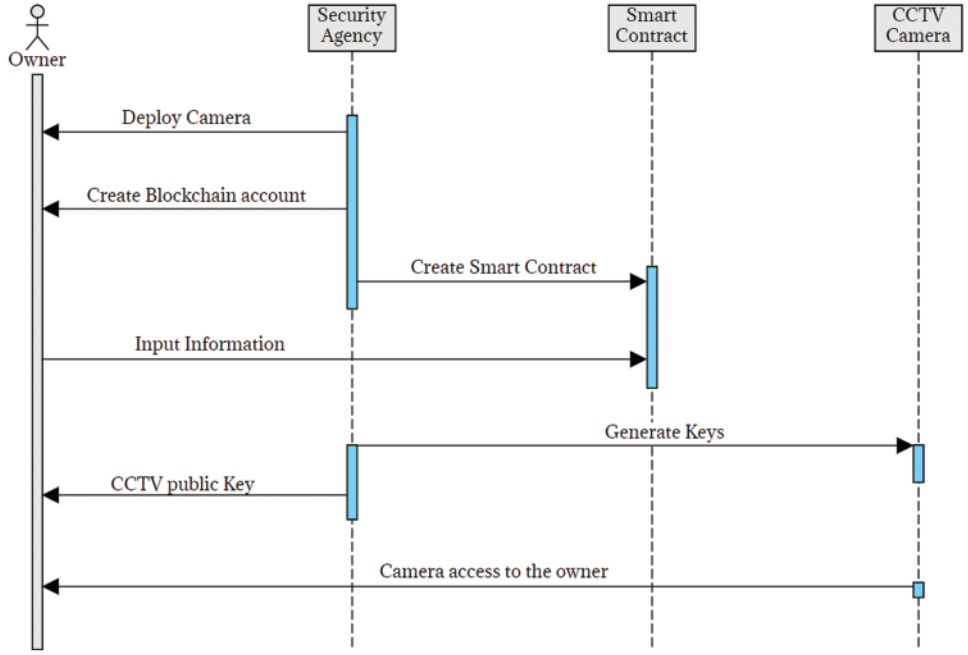

Figure 5: Deployment and smart contract creation

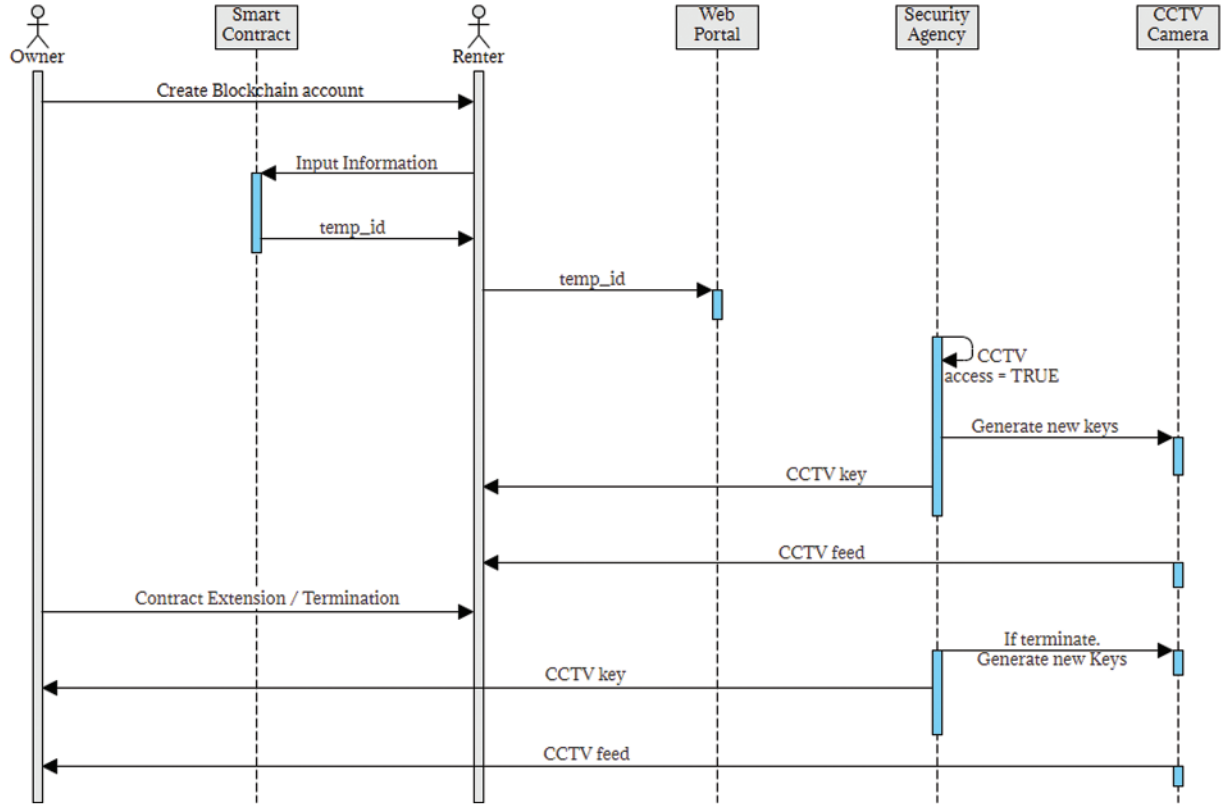

Figure 6: Renting property

After the new keys are generated, the CCTV security camera access to the owner is stopped, and the key is invalidated. The new public key of the CCTV camera is sent to the renter on their mobile number. This key remains with the renter until the rental contract expires, and they can have the CCTV security camera feed directed towards them uninterrupted. This is the part where the privacy feature of our proposed framework is preserved, and the security is ensured.

3.2.3 Expiration of Rental Contract

Fig. 6 shows the sequence of steps at the expiration of the rental contract. When the rental contract is about to expire, i.e., 1 day remaining in the duration entered in the smart contract, the user is prompted if the contract is to be extended or terminated. If the contract is extended, nothing is done, and the CCTV security camera feed continues. If the renter wants to terminate the contract, the security agency marks the CCTV security camera access as false and prompts the CCTV security camera to generate the new keys. At this point, the old keys get invalidated, and the CCTV stream to the renter stops. The security agency shares the new public key with the owner, and the stream is redirected to the owner.

3.3 Smart Contract

A novel smart contract algorithm is developed for this work. The algorithm works in three main parts where the conditions are executed. According to the system, there are multiple owners on the security agency's blockchain network with multiple properties, and each property has a separate smart contract and a single CCTV security camera. There can be one renter for a single property, and the multiple renters have an account on a blockchain network. The smart contract initially sets the expiry of contract as false since there is no contract yet. Also, the security agency keeps the CCTV security camera access as false.

Algorithm 1: Smart contract

Definitions: $O_i \in O$: Set of Owners
$R_i \in R$: Set of Renters
$SC_i \in SC$: Set of Smart Contracts
$P_i \in P$: Set of Properties of owners
SA: Security Agency
Input: Blockchain address and public key
Output: CCTV Camera feed redirection

Initialization: SC.expiry = false
SC.duration = renter defined
SA.CCTV_access = false
SA.CCTV_key = generate ( )
for each *Property* P_i, *Owner* O_i **do**
    Send O_i *[BC_addr, pub_key]* to SA
    $SA.P_i.temp\_id \leftarrow$ **NULL**
for each *Renter* R_i *after choosing property* $P_i \in P$ **do**
    Send R_i *[BC_addr, pub_key, ph_num]* to O_i
        O_i **generates** $O_i.temp\_id$
        $R_i.temp\_id \leftarrow O_i.temp\_id$
        $SA.P_i.temp\_id \leftarrow O_i.temp\_id$
    return $R_i.temp\_id$

(Continued)

Algorithm 1 (continued)

```
14  SA asks R_i to enter R_i.temp_id in the web browser
15      if R_i.temp_id == SA.P_i.temp_id
16          then
17              Set SA.CCTV_access == true
18              Set SC.expiry == true
19              SC.duration ← getRentDuration( )
20              return SA.CCTV_key to R_i
21  End
22      if SC.duration ≤ 1
23          then
24              R_i.ToExtendContract( )
25               if R_i.ToExtendContract == true
26                  then
27                     do nothing
28                  else
29                      Set SC.expiry == false
30                      Set SA.CCTV_access == false
31                      SA.CCTV_key ← generate( )
32                      Return access to O_i
33                  End
34  End
```

After the initialization and the generation of CCTV security camera's keys pair, the owner and the potential renter are asked to enter the details in the smart contract, shown in Lines 5–13. The security agency creates the temporary ID as NULL when the owners enter their details. When the renter sends their details to the owner, the owner generates a temporary ID based on the information. The owner sends this temporary ID to the renter and the security agency. Security agency updates the temporary ID from NULL. From Lines 14–21, the redirection of CCTV security camera's feed takes place from owner to the renter. Security agency asks the renter to enter the temporary ID on the web portal. The entered temporary ID is matched against the security agency's temporary ID. If the temporary ID matches, the renter is asked about the rental duration. The renter enters the duration to eliminate the chance of cheating by the owner to take more money for less duration. After the rental duration is entered, the *CCTV_access* and the *SC.expiry* are set to true. This is a call for the CCTV security camera to generate new keys pair. The new public key is sent to the renter, and the CCTV security camera feed is redirected to the renter for a specified time entered in the rental duration input. The expiration algorithm works in the same way as explained in the expiration of rental contract details and is shown in Lines 22–33. When the rental duration is about to expire (1 day remaining), the renter is asked if they want to extend the contract. If the contract is extended, nothing happens whereas, if the contract needs to be ended, the new keys pair for the CCTV security camera is generated. The new key is sent to the owner, and the CCTV security camera feed is redirected back.

Certain access control mechanisms are also part of the smart contract which restrict the continuous invocation of the smart contract leading to the collapse of the blockchain network. These include identity and role-based access control [45], attribute-based access control [46] and reputation-based access control [47]. In [45], the authors devise the design where IoT device and users are registered on the Distributed IDentity (DID) server and permissions in smart contract and access control are

granted based on the DID server control. Our system leverages from this design where the users, after creating the blockchain account and do the identity registration. The temp_id is sent to the registered users only and when the temp_id is validated on the security agency's web browser, the identity is verified again if the user is registered.

The overall flow of the SPAS architecture is shown in Fig. 7. This includes all the entities involved in the architecture whose details have been explained earlier. It shows all on-blockchain communication to and from the smart contract and all other off-chain blockchain communication with the dotted lines.

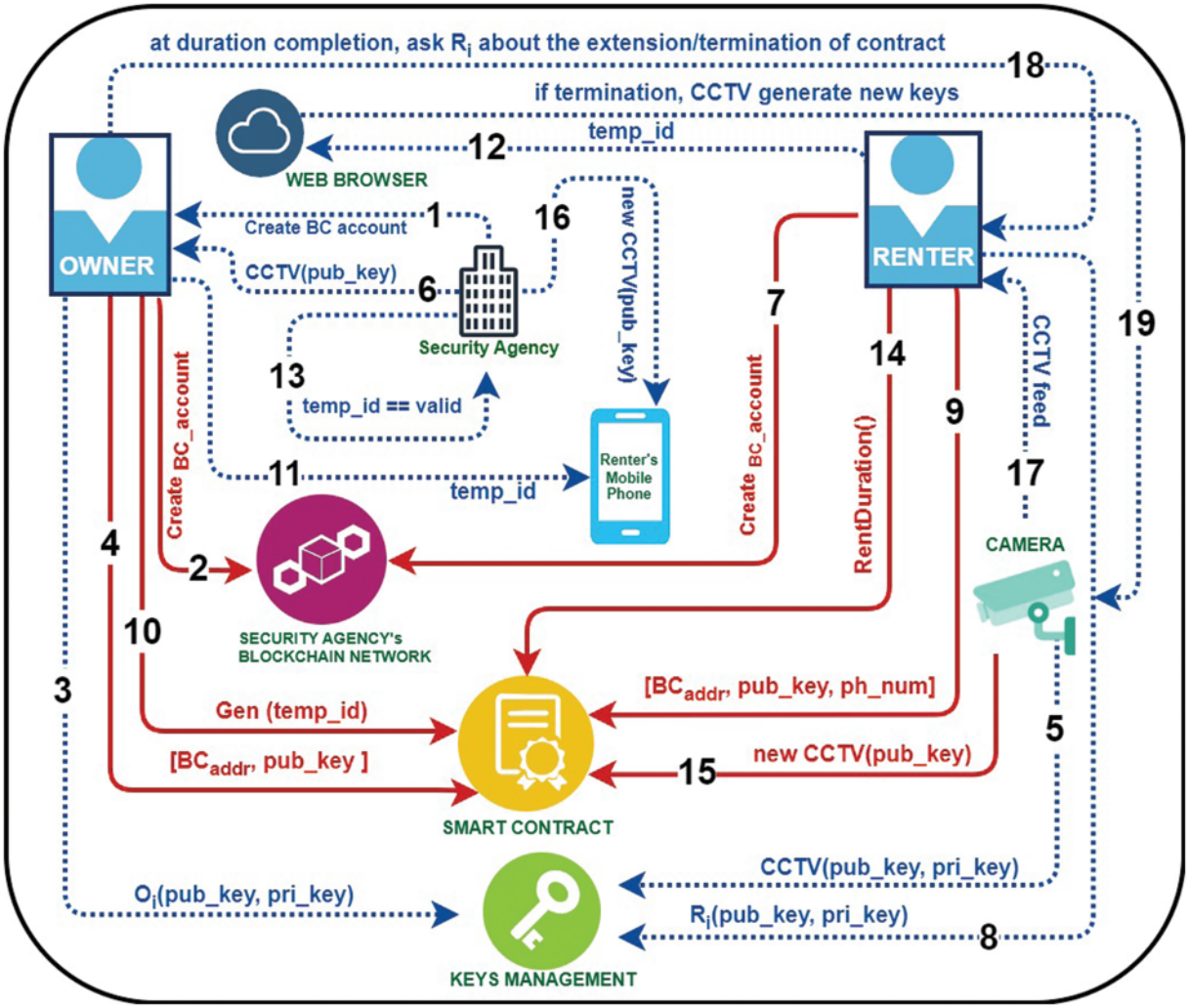

Figure 7: Flow of Secure Privacy and Anonymity Setup (SPAS) architecture

3.4 Keys Management

Keys management is part of the scheme where every entity involved in the system generates the public and private key pairs. In SPAS, we are generating the keys used by the owner, the renter, and the CCTV security camera. Multiple key generation algorithms have been developed over the period.

We have used the ring signature in our proposed scheme to maintain the anonymity of the owner and renter both.

We used the original ring signature, presented by Rivest, Shamir, and Tauman, with a slight modification. The three algorithms used for ring signature are *GEN*, *SIG*, and *VER*. The *GEN* algorithm remains the same, where the public and private keys are generated. The *SIG* algorithm creates the signature based on the ring of public keys of the participants of the ring and the private key of the original sender. It outputs a signature along with the key image, which is then verified in the *VER* algorithm, indicating the validity of the signature. This maintains anonymity throughout. Various versions of ring signatures have been worked upon. The multiple ring signatures approach is discussed in [48]. We have made a modification to the original ring signature where the message m can be signed by any member of the blockchain network who can be a non-member of the ring. In this way, the signer cannot be verified; else anyone with the key in R (public keys of the ring) can know that the signer is one of the ring members.

In ring signature, every ring participant signs the message using their public keys faking as their private keys while the original signer uses the original private key to generate the signature. Along with this signature, a key image is also generated which keeps the record as if the image has been consumed before or not. In this way, the issue of double spending is mitigated.

The modification to this scheme works in a scenario where one participant outside the ring can also sign the message with its public key. This is imagined as two rings in a ring signature. First, the members of the ring sign the message, then the outsider signs the already signed message. The original signers will not generate a signature again and the signature will be reused as explained in [49]. In this way no one in the ring may know who has signed the message as the original sender can be out of the ring too. As only one signer outside the ring can sign the message, this limit is kept in record to avoid too many signers from outside the ring. This modification enhances the level of anonymity in the system as another shield is put on the original signature. This is how anonymity works in the SPAS architecture. The security proof of the ring signature remains the same as [32], where we have added our modification.

- $GEN(1^k)$, where k is the security parameter.
- $SIG_{s,SK}(M,R)$ outputs the signature σ on the message M.
- $VER_R(M,\sigma)$ verifies the signature σ on a message M [32].

In addition to these algorithms, the fourth algorithm works for the signer from outside the ring. For simplicity, we denote it as $OSIG_{S',SK'}(\sigma, M, R)$ which outputs the signature σ'. A marker is embedded with the signature which ensures that the old ring members have already signed the message and cannot sign again and serves as a red flag. The resultant signature is the sum of both the first and second signatures as $\sigma + \sigma'$. The *VER* algorithm also works twice. First, it verifies that the signature σ is valid on the message M with respect to the ring R. If it is invalid, the *OSIG* outputs false, else it updates the signature with the outside member to σ'. Thus, the overall verification can be given as $((VER_R(\sigma) = 1) \wedge (VER_R(\sigma') = 1))$ to ensure the validity of the signature on message M with respect to the ring R. The security of the system is ensured as each ring signature of the two signatures in unforgeable [49].

Since the signer has legitimate access to every public key, this procedure eliminates the chance of creating an invalid public key. Based on the combination of these keys, they generate an authentic signature using their private key. Thus, the signature will be considered genuine without revealing the precise key that was used if the signer's private key is valid and matches one of the public keys. The security relies on the assumption that an honest participant owns at least one of the public keys in

the ring. The validity of the signature and the signer's anonymity are maintained if this requirement is met.

When it comes to the management of IoT devices on the blockchain, ring signatures can be applied in various ways to enhance privacy and security which include identity protection, anonymous transactions, group signatures, revocation and mixing services. In our framework, ring signatures add an extra layer of security to enhance the anonymity of the user through the modification made to the original ring signatures which allows one signer outside of the ring to participate. Furthermore, the revocation of old keys helps in ensuring the privacy of the owner or the renter.

4 Discussion and Analysis

Preserving privacy and maintaining anonymity is the prime focus of our proposed architecture. Privacy is preserved by using smart contract algorithm and unique key usage in the system at both the owner and the renter end. Anonymity on the other hand is maintained using the modified ring signature, leveraging from the original ring signature. With the use of both these mechanisms, security threats like double spending attacks, single point of failure attacks and private key attacks are mitigated. Limiting the attacks against these threats compared to the existing schemes proves the robustness of our architecture.

Different types of challenges were faced during the implementation phase of our system. The integration of on-blockchain and off-blockchain communication was one of them. Using online platforms like truffle suite and infura.io, we established our environment for the experiments. Another one was making a modification to the existing ring signature and getting the desired results. Leveraging from the original ring signatures mathematical modelling we made a modification to include our desired amendment. PyCryptodome is a self-contained python package of low-level cryptographic primitives and was used for making modifications to the existing ring signature.

Certain potential security concerns exist when it comes to IoT devices in context of blockchain integration like data privacy and central points of failure. The CCTV security camera system is built based on IoT-enabled technology. The security threats are eliminated by certain inclusions in the framework, like the multiple key generation process, eliminating the need for third-party and expiring the rental contract with old keys. Strong encryption and authentication are another security concern for blockchain-based IoT devices which is handled by using a modification to the existing ring signature.

4.1 Implementation

Our proposed scheme is an integration of multiple sections that are implemented as on-blockchain communication and off-blockchain communication together. On-blockchain communication represents the use of Ethereum and its smart contract. It helps to keep all the conditions pre-defined and keeps the legal aspects of the system intact. Transactions related to renting the CCTV security camera and maintaining the time of renting are maintained on-blockchain. This includes the renting details, CCTV security camera key exchange and the monetary transactions from renter to the owner. The Off-blockchain communication is carried out by the front-end development for the users which is implemented by Python3 and the Web3 library to make the calls between the users (owners and renters) and the security agency, the CCTV security camera and the security agency's web portal.

We used the Ethereum blockchain system through truffle suite and smart contracts as it gives the provision for adjusting the system to desired requirements. Truffle is a framework used for

Ethereum blockchain-based applications. It includes many features like smart contract development using solidity language, testing, migration scripts, and integration with other tools like IPFS. We used two 2.90 GHz CPUs and 16 GB memory and measured the key management, privacy, and anonymity level transaction times.

4.2 Key Management Analysis

Keys management is a complex stage that generates, verifies, and validates the keys for different entities in the system. This is an important part where the time taken is accumulated later in the transaction time and ultimately the block generation time. We compared the key management parameters with the PrC scheme, which uses zk-SNARK as a cryptographic technique. Our proposed SPAS system uses modified ring signatures, with lower proof complexity and better real-world usage. Both schemes are compared in key generation, proof generation, and verification times. Fig. 8 presents the comparison between PrC and SPAS. Key generation is the time taken to generate the key pairs while proof generation refers to building the signature. The verification time is the time taken to check the validity of the signature.

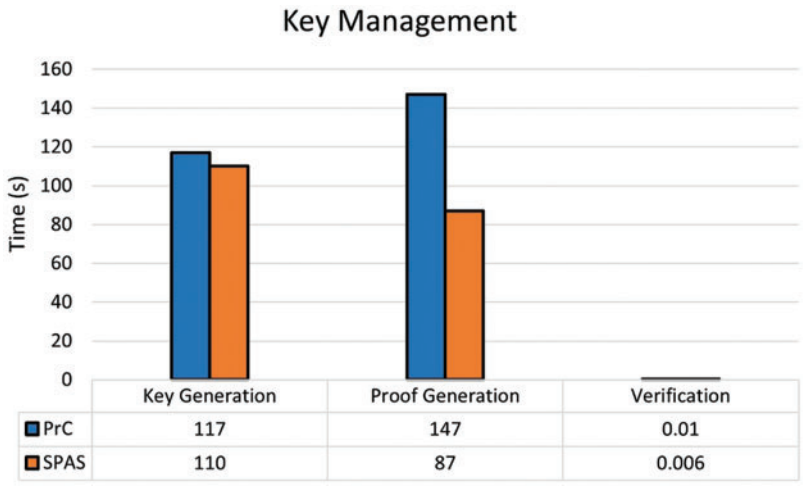

Figure 8: Key management analysis

4.3 Transactional Analysis

Transactions Per Second (TPS) refers to the rate at which a blockchain network can process transactions within a given second. The TPS metric provides an indication of the network's capacity to handle transactional throughput. However, the actual TPS of a blockchain can vary based on several factors like consensus mechanism, block size and time, scalability solutions and network design. In our proposed framework, the TPS decreases as the number of renters increases. This is because of the complex encryption scheme that takes more time for processing, which is then accumulated altogether and takes more transaction time. Therefore, the anonymity attribute comes with the tradeoff in form of scalability.

Another analysis is done regarding the privacy and anonymity level parameters between PrC and SPAS systems. For privacy analysis, we made comparisons in different parameters like confidentiality, proof complexity, and verification efficiency index. Fig. 9 shows the privacy level comparison between PrC and SPAS. PrC performs better in the confidentiality index as it uses a commitment scheme and

zk-SNARK, while the SPAS system uses a modified ring signature. The measuring parameter for confidentiality is the encryption strength. SPAS performs better in proof complexity and verification efficiency. Proof complexity is analyzed in terms of proof size while verification efficiency is analyzed by computational resources and scalability. The verification efficiency of ring signatures is better than the zk-SNARK as ring signature uses separate algorithms for each step.

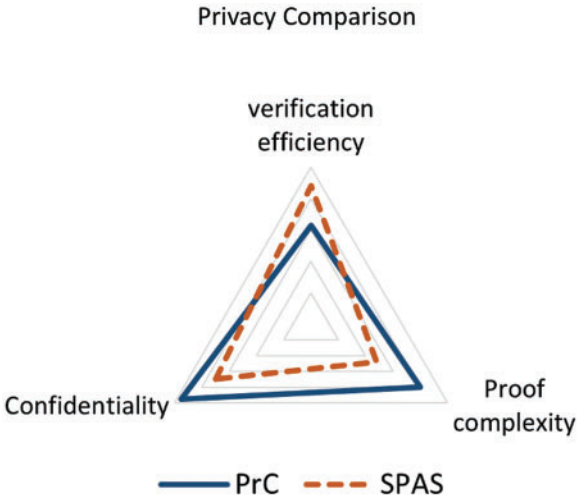

Figure 9: Privacy level comparison

For anonymity analysis, we compared PrC and SPAS systems for anonymity level, traceability resistance, and smart contracts integration. Fig. 10 shows the anonymity level comparison. In anonymity level and smart contracts integration, SPAS performs better than the PrC system due to the usage of ring signatures as compared to zk-SNARK. Anonymity level is analyzed by unlinkability and pseudonymity while smart contract integration is analyzed by functionality and use cases. The traceability resistance is analyzed by transaction privacy. The PrC performs better in traceability resistance since it is more complex due to using both the commitment scheme and zk-SNARK.

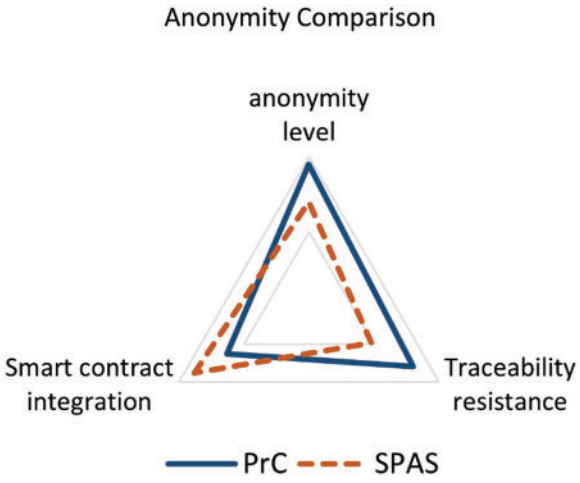

Figure 10: Anonymity level comparison

4.4 Comparative Analysis

We give a comparative analysis of SPAS with other schemes mentioned in Section 2. The parameters include privacy, anonymity, processing speed, smart contracts usage, and key usage. Below is Table 1 showing the comparative analysis. This comparison is done to show which scheme achieves the mentioned parameters completely or partially. It is important to show that our proposed architecture achieves the desired features in comparison with the existing schemes. This is due to the generation of new keys every time the tenant changes, which ensures privacy, and a modified ring signature which ensures anonymity.

Table 1: Comparative analysis

Categories	PETra	PrC	PP	SPAS
Privacy	Achieved	Achieved	Achieved	Achieved
Anonymity	Partially achieved	Achieved	Not achieved	Achieved
Speed	Slow due to routing	Slow due to masking	Slow due to messages	Slow due to ring signatures
Smart contract usage	No	No	Yes	Yes
Keys usage	Re-used	Re-used	Re-used	Always New

5 Conclusion

The SPAS architecture is specifically tailored to address concerns pertaining to privacy and anonymity within its existing design framework, effectively mitigating challenges associated with traceability and link-ability. The system employs a sophisticated mechanism, incorporating unique key utilization and key invalidation in conjunction with ring signatures. This amalgamation enhances the resilience of our scheme in preserving the anonymity of individuals. The applicability of this architecture extends beyond its current implementation, finding relevance in various IoT domains where privacy-sensitive data is at risk. Notably, in smart homes, the architecture safeguards data emanating from IoT devices, such as facial and voice recognition, by securely storing it on blockchain. Additionally, practical implications of this architecture manifest in the automotive sector, specifically through smart contracts facilitating smart car parking and fuel payments, ensuring the confidentiality of identity-sensitive and monetary transactions. A noteworthy contribution of our research is the introduction of a novel smart contract algorithm, notably characterized by the unique key usage architecture that enhances the efficiency of our system. The scalability of our system to diverse fields reliant on sensitive data, where the preservation of anonymity is imperative, underscores the versatility and relevance of our approach. Beyond IoT, the architecture finds potential implementation in the pharmaceutical industry, particularly in scenarios involving the development and distribution of drugs through wholesalers, dispensers, and end customers.

SPAS works in an efficient way but there exist some limitations. Latency is the issue that needs to be taken care of. When the scale of the system is expanded to scenarios like complete housing areas, delay can be a major issue. Since our scheme uses ring signature, which is computation intensive, the load of the system can make it slow. Another issue is the congestion at the blockchain due to the complexity of the encryption scheme used. The addition to the ring signature makes it more complex and it can cause congestion due to a lot of transactions together. In our future endeavors, we plan to implement this framework within the Hyperledger Fabric ecosystem, leveraging its modular

nature to seamlessly integrate our modular architecture. Furthermore, we aim to augment the privacy preservation capabilities of our system, enhancing its resilience against adversarial attacks. Lastly, our agenda includes expanding the application of our architecture to critical domains such as healthcare monitoring systems, where heightened security measures are paramount.

Acknowledgement: The authors wish to express their appreciation to the reviewers for their helpful suggestions which greatly improved the quality of this paper.

Funding Statement: This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) under the Artificial Intelligence Convergence Innovation Human Resources Development (IITP-2023-RS-2023-00255968) Grant and the ITRC (Information Technology Research Center) Support Program (IITP-2021-0-02051) funded by the Korea government (MSIT).

Author Contributions: The authors confirm contribution to the paper as follows: Study conception and design: M. Saad; data collection: M. Saad and M. R. Bhutta; analysis and interpretation of results: J. Kim and T. S. Chung; draft manuscript preparation: M. Saad and M. R. Bhutta. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Laszka, A. Dubey, M. A. Walker, and D. Schmidt, "Proving privacy, safety and security in IoT-based transactive energy systems using distributed ledgers distributed ledgers," in *Proc. IoT*, Linz, Austria, 2017, pp. 1–8.

[2] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Addressing security and privacy issues of IoT blockchain technology," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 881–888, 2021. doi: 10.1109/JIOT.2020.3008906.

[3] A. Pouraghily and T. Wolf, "A lightweight payment verification protocol for blockchain transactions on IoT," in *Proc. ICNC*, Honolulu, HI, USA, 2019, pp. 617–623.

[4] N. Saberhagen, "CryptoNote v2.0, white paper," *Computer Science*, 2013. Accessed: Dec. 16, 2022. [Online]. Available: https://cryptopapers.info/cryptonote/

[5] Q. Pan, J. Wu, A. K. Bashir, J. Li, S. Vashisht and R. Nawaz, "Blockchain and AI enabled configurable reflection resource allocation for IRS-aided coexisting drone-terrestrial networks," *IEEE Wirel. Commun.*, vol. 29, no. 6, pp. 46–54, 2022. doi: 10.1109/MWC.001.2200099.

[6] X. Lin, J. Wu, S. Mumtaz, S. Garg, J. Li and M. Guizani, "Blockchain-based on-demand computing resource trading in IoV-assisted smart city," *IEEE Trans. Emerg. Top. Comput.*, vol. 9, no. 3, pp. 1373–1385, 2020. doi: 10.1109/TETC.2020.2971831.

[7] N. Saquib, F. Bakir, C. Krintz, and R. Wolski, "A resource-efficient smart contract for privacy preserving smart home systems," in *Proc. SmartWorld/SCALCOM/UIC/ATC/SCI*, Atlanta, GA, USA, 2021, pp. 532–539.

[8] J. B. Liu, Y. Bao, and W. T. Zheng, "Analyses of some structural properties on a class of hierarchical scale-free networks," *Fractals*, vol. 30, no. 7, pp. 1–14, 2022. doi: 10.1142/S0218348X22501365.

[9] Q. Zhu, C. Xie, and J. B. Liu, "On the impact of the digital economy on urban resilience based on a spatial durbin model," *AIMS Math.*, vol. 8, no. 5, pp. 12239–12256, 2023. doi: 10.3934/math.2023617.

[10] G. N. Nguyen, N. H. L. Viet, M. Elhoseny, K. Shankar, B. B. Gupta and A. A. A. El-Latif, "Secure blockchain enabled cyber-physical systems in healthcare using deep belief network with ResNet model," *J. Parallel Distrib. Comput.*, vol. 153, no. 2, pp. 150–160, 2021. doi: 10.1016/j.jpdc.2021.03.011.
[11] Mamta, B. B. Gupta, K. C. Li, V. C. M. Leung, K. E. Psannis and S. Yamaguchi, "Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system," *IEEE/CAA J. Autom. Sin.*, vol. 8, no. 12, pp. 1877–1890, 2021. doi: 10.1109/JAS.2021.1004003.
[12] C. Manthiramoorthy, K. M. S. Khan, and A. N. Ameen, "Comparing several encrypted cloud storage platforms," *Int. J. Math. Comput. Sci.*, vol. 2, pp. 44–62, 2024. doi: 10.59543/ijmscs.v2i.7971.
[13] P. Mendki, "Blockchain enabled IoT edge computing: Addressing privacy, security and other challenges," in *Proc. ICBCT'20*, Hilo, USA, 2020, pp. 63–67.
[14] R. Kumar, S. Singh, and K. T. Chui, "A novel decentralized group key management scheme for cloud-based vehicular IoT networks," *Int. J. Cloud Appl. Comput.*, vol. 12, no. 1, pp. 1–34, 2022. doi: 10.4018/IJCAC.
[15] A. Raj and S. Prakash, "A privacy-preserving authentic healthcare monitoring system using blockchain," *Int. J. Software Sci. Comput. Intell.*, vol. 14, no. 1, pp. 1–23, 2022. doi: 10.4018/IJSSCI.
[16] A. Fitwi and Y. Chen, "Secure and privacy-preserving stored surveillance video sharing a top permissioned blockchain," in *Proc. ICCCN*, Athens, Greece, 2021, pp. 1–8.
[17] P. W. Khan, Y. C. Byun, and N. Park, "A data verification system for CCTV surveillance cameras using blockchain technology in smart cities," *Electronics*, vol. 9, no. 3, pp. 1–21, 2020. doi: 10.3390/electronics9030484.
[18] M. O. Okoye and H. M. Kim, "Optimized user-friendly transaction time management in the blockchain distributed energy market," *IEEE Access*, vol. 10, pp. 34731–34742, 2022. doi: 10.1109/ACCESS.2022.3162214.
[19] V. Rajinikanth, S. Yassine, and S. A. Bukhari, "Hand-sketchs based parkisnson's disease screening using lightweight deep-learning with two-fold training and fused optimal features," *Int. J. Math., Stat. Comput. Sci.*, vol. 2, pp. 9–18, 2024. doi: 10.59543/ijmscs.v2i.7821.
[20] P. Zhu, J. Hu, Y. Zhang, and X. Li, "Enhancing traceability of infectious diseases: A blockchain-based approach," *Inf. Process. Manage.*, vol. 58, no. 4, pp. 102570, 2021. doi: 10.1016/j.ipm.2021.102570.
[21] J. Hu, P. Zhu, Y. Qi, Q. Zhu, and X. Li, "A patent registration and trading system based on blockchain," *Expert Syst. Appl.*, vol. 201, no. 1, pp. 117094, 2022. doi: 10.1016/j.eswa.2022.117094.
[22] P. Zhu, J. Hu, X. Li, and Q. Zhu, "Using blockchain technology to enhance the traceability of original achievements," *IEEE Trans. Eng. Manag.*, vol. 70, no. 5, pp. 1693–1707, 2023. doi: 10.1109/TEM.2021.3066090.
[23] Y. Cai, W. Ke, E. Cui, and F. Yu, "A deep recommendation model of cross-grained sentiments of user reviews and ratings," *Inf. Process. Manage.*, vol. 59, no. 2, pp. 102842, 2022. doi: 10.1016/j.ipm.2021.102842.
[24] P. Zhu, C. Miao, Z. Wang, and X. Li, "Informational cascade, regulatory focus and purchase intention in online flash shopping," *Electron. Commer. Res. Appl.*, vol. 62, no. 6, pp. 101343, 2023. doi: 10.1016/j.elerap.2023.101343.
[25] S. Banupriya and K. Kottilingam, "An analysis of privacy issues and solutions in public blockchain (Bitcoin)," in *Proc. INCET*, Belagavi, India, 2021, pp. 1–7.
[26] M. Kashif and K. Kalkan, "BCPriPIoT: Blockchain utilized privacy-preservation mechanism for IoT devices," in *Proc. BCCA*, Tartu, Estonia, 2021, pp. 201–208.
[27] M. N. Islam and S. Kundu, "Poster abstract: Preserving IoT privacy in sharing economy via smart contract," in *Proc. IoTDI*, Orlando, FL, USA, 2018, pp. 296–297.
[28] X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, "A blockchain privacy protection scheme based on ring signature," *IEEE Access*, vol. 8, pp. 76765–76772, 2020. doi: 10.1109/ACCESS.2020.2987831.
[29] J. Berquist, A. Laszka, M. Sturm, and A. Dubey, "On the design of communication and transaction anonymity in blockchain-based transactive microgrids," in *Proc. SERIAL*, NewYork, NY, USA, 2017, pp. 1–6.
[30] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. PerCom Workshops*, Kona, USA, 2017, pp. 618–623.

[31] Y. Long, Y. Chen, W. Ren, H. Dou, and N. N. Xiong, "DePET: A decentralized privacy-preserving energy trading scheme for vehicular energy network via blockchain and K-anonymity," *IEEE Access*, vol. 8, pp. 192587–192596, 2020. doi: 10.1109/ACCESS.2020.3030241.
[32] A. Bender, J. Katz, and R. Morselli, "Ring signatures: Stronger definitions, and construction with random oracles," in *Proc. TCC*, Berlin, Germany, 2006, pp. 60–79.
[33] R. Crammer, I. Damgard, and B. Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocol," in *Proc. AICC*, Santa Barbara, California, USA, 1994, pp. 174–187.
[34] L. Xu *et al.*, "Enabling the sharing economy: Privacy respecting contract based on public blockchain," in *Proc. BCC*, New York, NY, USA, 2017, pp. 15–21.
[35] D. A. Luong and J. H. Park, "Privacy-preserving identity management system on blockchain using Zk-SNARK," *IEEE Access*, vol. 11, pp. 1840–1853, 2023. doi: 10.1109/ACCESS.2022.3233828.
[36] M. A. Islam and S. Madria, "A permissioned blockchain based access control system for IoT," in *Proc. Blockchain*, Atlanta, GA, USA, 2019, pp. 469–476.
[37] X. Liu, M. Zhang, Y. Zheng, and Y. Yang, "A linkable ring signature electronic cash scheme based on blockchain," in *Proc. SmartBlock*, Zhengzhou, China, 2020, pp. 1–4.
[38] Y. Jeong, D. Y. Hwang, and K. H. Kim, "Blockchain-based management of video surveillance systems," in *Proc. ICOIN*, Kuala Lumpur, Malaysia, 2019, pp. 465–468.
[39] A. Pouraghily, M. N. Islam, S. Kundu, and T. Wolf, "Poster abstract: Privacy in blockchain-enabled IoT devices," in *Proc. IoTDI*, Orlando, FL, USA, 2018, pp. 292–293.
[40] M. Shurman, A. A. Obeidat, and S. A. Shurman, "Blockchain and smart contract for IoT," in *Proc. ICICS*, Irbid, Jordan, 2020, pp. 361–366.
[41] A. R. Mahlous and A. Ara, "The adoption of blockchain technology in IoT: An insight view," in *Proc. CDMA* , Riyadh, Saudi Arabia, 2020, pp. 100–105.
[42] M. Shanker, "Use case: Smart contracts for lease agreements using blockchain technology," *Int. J. Sci. Res. Comput. Sci. Eng.*, vol. 7, no. 6, pp. 1–9, 2019. doi: 10.26438/ijsrcse/v7i6.19.
[43] N. Chaudhry and M. M. Yousaf, "Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities," in *Proc. ICOSST*, Lahore, Pakistan, 2018, pp. 54–63.
[44] Y. N. Aung and T. Tantidham, "Review of ethereum: Smart home case study," in *Proc. INCIT*, Nakhon-pathom, Thailand, 2017, pp. 1–4.
[45] Y. Ma, Y. Fu, L. Liu, Z. Du, J. Ma and Y. Sun, "A smart contract approach to access control based on distributed identities and roles," in *Proc. ICITBS*, Hengyang, China, 2022, pp. 677–680.
[46] L. Song, Z. Zhu, M. Li, L. Ma, and X. Ju, "A novel access control for Internet of Things based on blockchain smart contract," in *Proc. IAEAC*, Chongqing, China, 2021, pp. 111–117.
[47] Q. Chen, H. Zhao, P. Feng, and W. Jiao, "Smart contracts and reputation-based access control solutions for the Internet of Things," in *Proc. ISPDS*, Guangzhou, China, 2023, pp. 651–656.
[48] R. Tso, X. Yi, T. Ito, T. Okamoto, and E. Okamoto, "Design and analysis of "flexible *k*-out-of-*n* signatures," in *Proc. Autonomic and Trusted Computing (ATC)*, Xi'an, China, 2010, pp. 255–267.
[49] T. Okamoto, R. Tso, M. Yamaguchi, and E. Okamoto, "A *k*-out-of-*n* ring signature with flexible participation for signers," *Cryptology ePrint*, 2018. Accessed: Jun. 22, 2023. [Online]. Available: http://eprint.iacr.org/2018/728